

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Teknologi masa kini telah berkembang kian pesat, diawali dengan munculnya berbagai teknologi di bidang ICT, khususnya pada sistem jaringan komputer, baik dari segi kompleksitas maupun ukurannya. Namun demikian, hal ini tidak mengurangi kerentanannya terhadap serangan. Berdasarkan statistik yang diperoleh, tingkat eksploitasi jaringan komputer semakin tinggi. Hal ini seiring dengan meningkatnya pengetahuan, teknik, dan *tools* yang dipakai dalam melakukan penyerangan. Bahkan orang awam pun dapat dengan mudah menggunakan *tools* yang ada untuk melakukan penetrasi ke sebuah sistem.

Teknologi yang digunakan untuk menangkal serangan tersebut sebenarnya telah ada, namun perkembangannya telah mencapai batas. Penggunaan teknologi tersebut menjadi tidak efisien karena tidak dapat menjamin keakuratan keamanannya. Salah satu teknik yang digunakan adalah Intrusion Detection Systems (IDS) yang digunakan untuk mendeteksi serangan. Namun, adakalanya IDS ini tidak mampu mendeteksi paket – paket yang tidak sah karena tingginya trafik dalam jaringan. Untuk mengatasi kelemahan dari IDS itu maka dikembangkan suatu teknik yang disebut *honeypot*.

Honeypot merupakan suatu sistem yang sengaja dirancang untuk diserang, namun tidak menyediakan layanan dari sistem tersebut. Tujuan dari pembuatan *honeypot* ini adalah untuk mengelabui penyerang sehingga mendapatkan informasi yang akurat dari pihak penyerang. Trafik yang berasal atau menuju ke *honeypot* dipastikan tidak sah sehingga dari trafik ini dapat diperoleh informasi baik berupa metode, *tools*, maupun alamat dari penyusup.

Tugas akhir ini akan membahas mengenai implementasi *honeypot* pada layanan VoIP, dimana serangan pada VoIP kini semakin meningkat, seperti serangan *DOS (Denial of Service)* yang dapat mengganggu kualitas layanan yang diberikan. Untuk mengatasi hal tersebut maka pada jaringan VoIP akan diintegrasikan dengan sebuah *honeypot*. Disamping itu, pola serangan yang

diperoleh pada *log honeypot* pun dapat dijadikan acuan untuk perbaikan sistem pertahanan yang telah ada, seperti *firewall* ataupun IDS.

1.2 Maksud dan Tujuan

Tujuan dari penelitian tugas akhir ini adalah

1. Mengimplementasikan honeypot pada layanan VoIP.
2. Menganalisis kinerja dari honeypot yang telah diimplementasikan.
3. Mengimplementasikan IDS dan firewall pada layanan VoIP.
4. Menganalisis kinerja dari IDS dan firewall yang telah diimplementasikan.

1.3 Rumusan Masalah

Permasalahan yang dijadikan obyek penelitian dan pengembangan pada tugas akhir ini adalah :

1. Bagaimana membangun sebuah honeypot pada jaringan VoIP.
2. Bagaimana mengalihkan trafik yang tidak sah ke honeypot.
3. Bagaimana menyimpan log file penyusup pada honeypot.
4. Bagaimana membangun sebuah gateway firewall dan IDS pada jaringan VoIP.
5. Bagaimana mengintegrasikan honeypot dengan IDS dan firewall.

1.4 Batasan Masalah

Batasan masalah dalam penelitian dan pengembangan pada tugas akhir ini adalah:

1. Implementasi dan pengujian jaringan dilakukan di laboratorium
2. Aspek yang akan dianalisis adalah access control, availability, confidentiality, dan integrity.
3. Hanya membahas pada ipv4.
4. Tidak membahas algoritma pemrograman honeypot.
5. Codec yang digunakan G.711.

6. Komunikasi yang dilakukan adalah komunikasi suara dengan menggunakan *Trixboxserver* dan *SIP (Session Initiation Protocol)* sebagai protokol pensinyalannya.
7. Client VoIP berupa sebuah *PC* yang dilengkapi dengan software *X-Lite*.
8. Percobaan yang dilakukan dalam lingkup user mode linux.
9. Engine signature-based IDS yang digunakan adalah *Snort*.
10. Engine honeypot yang digunakan adalah *artemisa*.
11. Firewall yang digunakan adalah *iptables* dengan kernel linux ubuntu.
12. Skema pengumpulan informasi berupa *network based information gathering*.
13. Level interaksi honeypot yang dipakai *mid-interaction honeypot*.
14. Jenis honeypot yang diimplementasikan berupa *production honeypot*.

1.5 Metode Penelitian

Metode penelitian yang digunakan pada tugas akhir ini adalah:

1. Studi literatur
Mempelajari konsep dan dasar teori yang berhubungan dengan tugas akhir ini, diantaranya konsep Honeypot, VoIP, firewall dan IDS.
2. Perancangan dan implementasi sistem
Pada tahap ini dilakukan perancangan jaringan dan implementasinya, dimulai dari mencari bahan-bahan yang berkaitan, memilih beberapa dari banyak pilihan *software*, dan mencobanya di laboratorium.
3. Analisis
Pada tahap ini dilakukan analisis terhadap jaringan honeypot yang telah dibuat, terutama kemampuan fingerprintnya.
4. Penarikan kesimpulan

Dari semua tahap selama pengerjaan tugas akhir, diambil kesimpulan berdasarkan tujuan pengerjaan tugas akhir ini.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini terbagi dalam beberapa bagian yaitu:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, maksud dan tujuan, perumusan masalah penelitian, batasan masalah, metode penelitian dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini berisi dasar teori yang berkaitan dengan tugas akhir ini, seperti berbagai hal tentang honeypot, VoIP, snort, serta *firewall*.

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM

Bab ini berisi model perancangan sistem yang dibuat serta langkah-langkah dalam implementasinya honeypot pada layanan VoIP.

BAB IV ANALISIS

Pada bab ini akan dilakukan uji coba berdasarkan parameter – parameter yang telah ditetapkan, dan kemudian dilakukan analisis terhadap hasil uji coba tersebut serta pengukuran kinerja sistem.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan serta saran dari seluruh kegiatan penelitian tugas akhir ini untuk pengembangan selanjutnya.